System Assessment and Validation for Emergency Responders (SAVER)

Common Alerting Protocol
Alert Origination Tools
Technology Guide

February 2015

Homeland Security
Science and Technology

U.S. Department of Homeland Security
SAVER
System Assessment and Validation for Emergency Responders

Prepared by Space and Naval Warfare Systems Center Atlantic

The *Common Alerting Protocol Alert Origination Tools Technology Guide* was funded under Interagency Agreement No. HSHQPM-13-X-00024 from the U.S. Department of Homeland Security, Science and Technology Directorate.

The views and opinions of authors expressed herein do not necessarily reflect those of the U.S. Government.

Reference herein to any specific commercial products, processes, or services by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government.

The information and statements contained herein shall not be used for the purposes of advertising, nor to imply the endorsement or recommendation of the U.S. Government.

With respect to documentation contained herein, neither the U.S. Government nor any of its employees make any warranty, express or implied, including but not limited to the warranties of merchantability and fitness for a particular purpose. Further, neither the U.S. Government nor any of its employees assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed; nor do they represent that its use would not infringe privately owned rights.

The cover photo was provided by Space and Naval Warfare Systems Center Atlantic.

FOREWORD

The U.S. Department of Homeland Security (DHS) established the System Assessment and Validation for Emergency Responders (SAVER) Program to assist emergency responders making procurement decisions. Located within the Science and Technology Directorate (S&T) of DHS, the SAVER Program conducts objective assessments and validations on commercially available equipment and systems, and develops knowledge products that provide relevant equipment information to the emergency responder community. The SAVER Program mission includes:

- Conducting impartial, practitioner-relevant, operationally oriented assessments and validations of emergency response equipment; and
- Providing information, in the form of knowledge products, that enables decision-makers and responders to better select, procure, use, and maintain emergency response equipment.

SAVER Program knowledge products provide information on equipment that falls under the categories listed in the DHS Authorized Equipment List (AEL), focusing primarily on two main questions for the responder community: “What equipment is available?” and “How does it perform?” These knowledge products are shared nationally with the responder community, providing a life- and cost-saving asset to DHS, as well as to Federal, state, and local responders.

The SAVER Program is supported by a network of Technical Agents who perform assessment and validation activities. As a SAVER Program Technical Agent, the Space and Naval Warfare Systems Center (SPAWARSYSCEN) Atlantic has been tasked to provide expertise and analysis on key subject areas, including communications, sensors, security, weapon detection, and surveillance, among others. In support of this tasking SPAWARSYSCEN Atlantic developed this technology guide to provide emergency responders with information on the Integrated Public Alert and Warning System alert origination tools, which fall under AEL reference number 04AP-09-ALRT titled Systems, Public Notification and Warning.

Visit the SAVER Website on First Responder.gov (http://www.firstresponder.gov/SAVER) for more information on the SAVER Program or to view additional reports on alert and warning systems or other technologies.

POINTS OF CONTACT

SAVER Program
U.S. Department of Homeland Security
Science and Technology Directorate
FRG Stop 0203
245 Murray Lane
Washington, DC 20528-0215

E-mail: saver@hq.dhs.gov
Website: http://www.firstresponder.gov/SAVER

Space and Naval Warfare Systems Center Atlantic
Advanced Technology and Assessments Branch
P.O. Box 190022
North Charleston, SC 29419-9022

E-mail: ssc_lant_saver_program.fcm@navy.mil

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. INTRODUCTION

The Integrated Public Alert and Warning System (IPAWS) is the latest system designed to enable the President of the United States to warn the American public of emergencies and disasters. The primary objective of IPAWS is to modernize and integrate existing alert and warning systems at the national, state, territorial, local, and tribal levels in a single, cohesive interface. IPAWS is developed, implemented, and managed by the Federal Emergency Management Agency (FEMA) in partnership with the Federal Communications Commission (FCC) and the U.S. Department of Commerce's National Oceanic and Atmospheric Administration (NOAA).

While IPAWS is not mandatory, many emergency response agencies are working to adopt IPAWS in their jurisdictions. The system provides a means to alert citizens through multiple communications methods simultaneously, requiring composition of only one alert message and increasing the likelihood that the message will successfully reach the public. The messaging tools employed by agencies to send and receive IPAWS messages are an important implementation consideration and are the focus of this document.

The System Assessment and Validation for Emergency Responders (SAVER) Program developed this technology guide to provide an overview of:

- The messaging tools emergency responders can employ to send and receive emergency messages through IPAWS;
- IPAWS's technology, architecture, components, and standards with regards to those tools and their use; and
- The process agencies can follow to implement IPAWS.

This document is based on information gathered from March to November 2014 from Internet research, industry publications, and subject matter experts.

2. IPAWS TECHNOLOGY OVERVIEW

IPAWS leverages public alerting systems already established and evolving at the national and local level, summarized in Table 2-1, by providing a framework of servers, software, and standard formats that connect alert origination points (i.e., agencies issuing an alert) with existing public alerting systems through modern transmission means. This system is called IPAWS Open Platform for Emergency Networks (IPAWS-OPEN). The primary messaging standard employed by IPAWS is the Common Alerting Protocol (CAP™), which provides a consistent format for emergency messages distributed by the system. CAP also presents an opportunity to enhance emergency message delivery to all Americans inclusive of Americans with disabilities and Americans with access and functional needs, in accordance with Executive Order 13407.

Table 2-1. Public Alerting Systems

System	Dissemination Means	Implementor
Emergency Alert System (EAS)	Audio and text-based messages pushed to radio and television	FCC/FEMA/NOAA
Wireless Emergency Alerts (WEA)	Text-based messages pushed to cellular devices	FCC/FEMA/Cellular carriers
NOAA Weather Radio All Hazards via HazCollect	Radio broadcasts in the VHF public service frequency band between 162.400 and 162.550	NOAA
Internet		
Websites and applications	Messages posted or popped up on organizational websites	Individual agency
Applications accessing social media networks	Messages posted on organizational social networking sites	Individual agency
Online gaming systems	Messages pushed to gaming screens	Individual agency
Instant messaging	Text-based messages pushed to computers	Individual agency
Unique Alerting Systems		
Siren systems	Auditory sirens, horns, and voice playback	Individual agency
Emergency telephone networks	Voice messages	Individual agency
Digital road signs	Text-based messages	Individual agency
FM Radio Broadcast Data Systems (RBDS)	Text-based messages	Individual agency
E-mail and Short Message Service (SMS) Subscription Services	Text-based messages	Individual agency

2.1 IPAWS Architecture

The IPAWS architecture is shown in Figure 2-1 and can be accessed from the IPAWS Website at the Informational Materials Page. The process begins when an alerting authority wishes to compose an emergency message for dissemination within the target community. The message is composed using a CAP Alert Origination Tool, a software program commonly referred to as a messaging or CAP tool. Then the message is transmitted over the Internet to IPAWS-OPEN where it is authenticated and checked for proper format and permissions. At this point, IPAWS-OPEN sends the message to the appropriate public alerting systems, such as Emergency Alert System (EAS) and Wireless Emergency Alerts (WEA). These systems then send the message through the applicable communications media where it can be seen or heard by community members in the target geographic area.

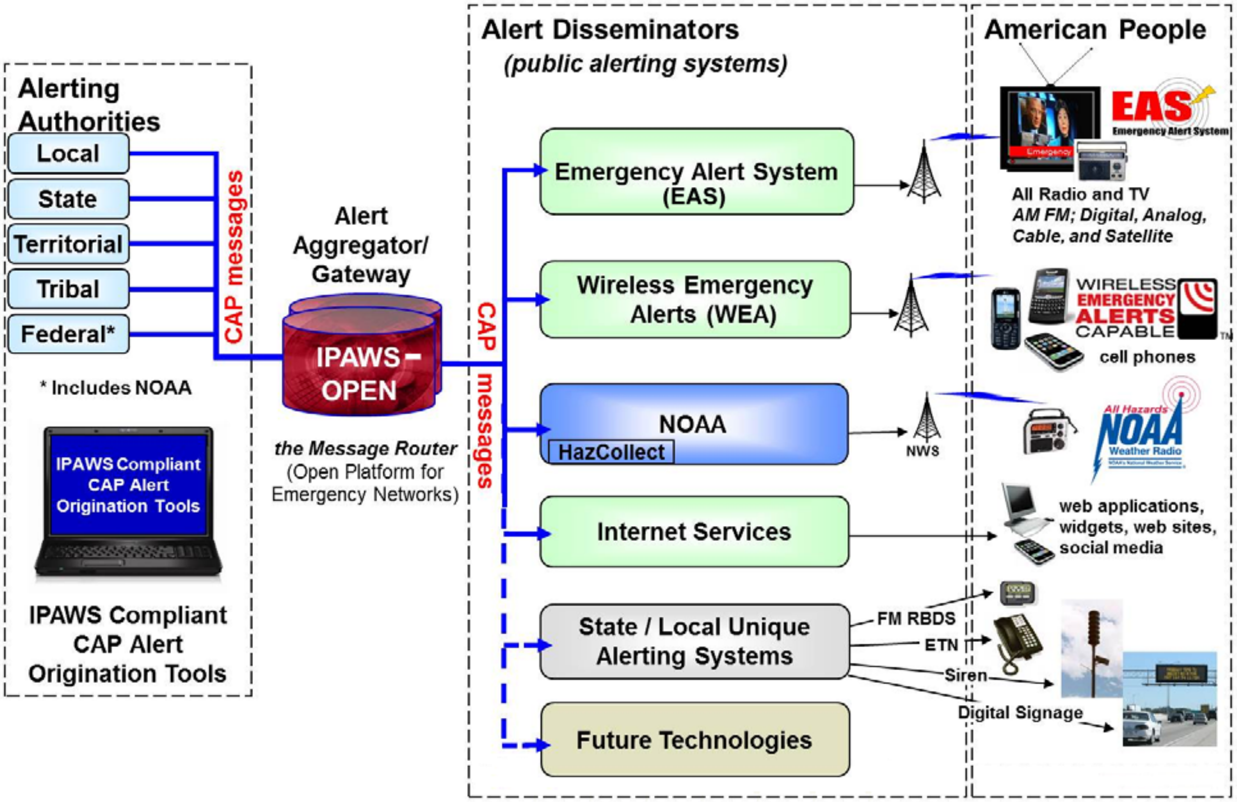

Alerting Authorities
Local
State
Territorial
Tribal
Federal*
* Includes NOAA
CAP messages
IPAWS Compliant CAP Alert Origination Tools
IPAWS Compliant CAP Alert Origination Tools
Alert Aggregator/ Gateway
IPAWS-OPEN
the Message Router (Open Platform for Emergency Networks)
CAP messages
Alert Disseminators (public alerting systems)
Emergency Alert System (EAS)
Wireless Emergency Alerts (WEA)
NOAA
HazCollect
NWS
Internet Services
State / Local Unique Alerting Systems
FM RBDS
ETN
Siren
Digital Signage
Future Technologies
American People
EAS Emergency Alert System
All Radio and TV AM FM; Digital, Analog, Cable, and Satellite
WIRELESS EMERGENCY ALERTS CAPABLE
cell phones
All Hazards NOAA Weather Radio
web applications, widgets, web sites, social media

Figure 2-1. IPAWS Architecture Diagram

Image courtesy of FEMA

2.2 IPAWS Components

IPAWS is comprised of the systems and devices described in the following sections.

2.2.1 CAP Alert Origination Tools

CAP Alert Origination Tools are software programs that provide alerting authorities the ability to compose, send, and receive CAP-based messages through IPAWS. Software may be installed in three basic ways: on server hardware in a vendor-managed data center, on server hardware in the agency's own data center, or on a single computer with access to the Internet. These tools are discussed further in Section 3.

Additional information regarding the installation methods for IPAWS Compliant CAP Alert Origination Tools can be found in the *Study of Integration Strategy Considerations for Wireless Emergency Alerts* report located in the Document Library on FirstResponder.gov.

2.2.2 IPAWS Open Platform for Emergency Networks

IPAWS-OPEN is a FEMA-managed system that aggregates, authenticates, and disseminates messages simultaneously to multiple public alerting systems. IPAWS-OPEN acts as a CAP message broker and dissemination gateway for emergency information going out over public communications networks or from one IPAWS user to another.

Emergency messages sent by alerting authorities are posted to IPAWS-OPEN. The sender's digital signature is first authenticated by IPAWS-OPEN. Next, the message format is validated to ensure that it is in a valid CAP format. Finally, permissions for the sender are verified to ensure the sender is authorized to send that type of alert to the identified geographic region and the sender has approved access to the alerting systems indicated in the CAP message.

The message is then distributed to the systems indicated (e.g., EAS, WEA) in the CAP message. Further, the message is made available via the IPAWS All-Hazards Alert Feed, which can be queried or "polled" by an agency for any relevant messages.

Information on IPAWS-OPEN can be found on the IPAWS Website.

2.2.3 Existing National Public Alerting Systems

IPAWS-OPEN communicates with existing national public alerting systems, such as EAS, WEA, and NOAA's HazCollect, to disseminate emergency messages to the affected geographic locations.

Emergency Alert System (EAS)

The EAS is part of IPAWS. It is a legacy system jointly coordinated by FEMA, the FCC, and broadcasters, in partnership with public and private service providers (called EAS participants), that sends emergency alerts through radio and television channels. The system's primary purpose is to provide the President of the United States with a means to deliver national alerts. Broadcast radio may be the only communications media platform still operational and accessible using car, hand-crank, or battery-operated radios when electrical power and communications systems are degraded or unavailable. Therefore, EAS remains a core public alerting system for IPAWS. EAS pathways include:

- Analog radio and television;
- Wired and wireless cable television;
- Direct broadcast satellite;
- Digital television;
- Satellite digital audio radio service;
- Digital cable;
- Digital audio broadcast; and
- Wireline video.

EAS employs a messaging protocol developed for NOAA Weather Radio (NWR), called Specific Area Message Encoding (SAME), to create and issue alert messages. The FCC now requires EAS participants to be capable of processing CAP-formatted alert messages from IPAWS. In order to comply with FCC regulations, EAS participants must have an Internet connection and CAP-compliant EAS equipment. The equipment, which translates CAP messages to the EAS/SAME protocol and message format, can consist of firmware upgrades to existing encoder/decoders, new encoder/decoder models with CAP fully integrated, or stand-alone converters. This allows alerting authorities to activate the EAS through IPAWS-OPEN.

When IPAWS-OPEN authenticates and validates a message received for dissemination over EAS, it posts the message to the IPAWS EAS Feed. EAS participants monitor or poll the feed with their IPAWS compatible equipment through an Internet connection. According to FEMA, there are approximately 20,000 EAS participants who are required to monitor the IPAWS All-Hazards Alert Feed. When an active CAP message fitting the station's profile is detected, the equipment determines the required action as specified in the message. These actions typically include generating an EAS alert, processing the audio as directed in the message, and sending the EAS message, which results in an interruption of radio and television programming in the area in order to issue the auditory or text-based message. EAS participants also monitor the emergency information sources detailed in their EAS Plan, such as state/local EAS servers, local NWR broadcasts, and local Primary Entry Point (PEP) radio stations, for relevant messages that need to be disseminated.

PEP stations, like the one shown in Figure 2-2, act as relay points for Presidential alerts over EAS. PEPs are private or commercial radio stations participating with FEMA to issue alert and warning information, both national and local, before, during, and after an emergency. Although EAS is a national system, FEMA encourages state, local, territorial, and tribal alerting authorities to coordinate with local PEPs for dissemination of their alerts when possible. FEMA is executing an expansion and modernization program to increase the number of PEP radio stations and upgrade them with specialized capabilities, such as redundant communications equipment, an IPAWS compatible EAS receiver, modernized data transmission options, and emergency power generators. This enables dissemination of emergency information via IPAWS even in the event of power loss. FEMA's goal is to have 77 PEPs operational by 2015, which will provide direct coverage to over 90 percent of the population.

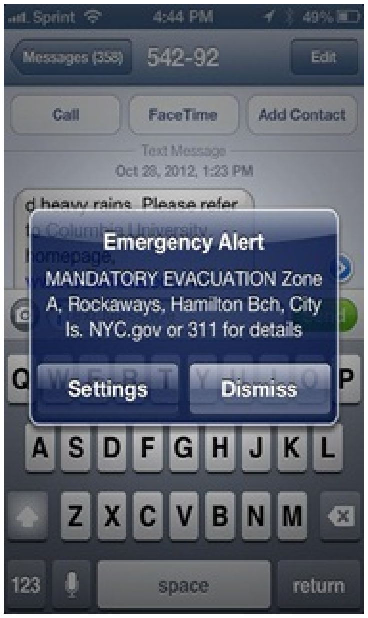
Figure 2-2. PEP Station

Image courtesy of FEMA

Information on EAS can be found on the IPAWS Website.

Wireless Emergency Alerts (WEA)

The WEA system, formerly known as the Commercial Mobile Alert System or CMAS, is also part of IPAWS. WEA is an initiative by the FCC, in partnership with FEMA and volunteer cellular carriers, to provide a system that can broadcast 90-character emergency messages to WEA-enabled cellular phones within a designated geographic area. WEA can be activated by all government alerting authorities, as well as the National Weather Service (NWS) and National Center for Missing and Exploited Children (NCMEC), through IPAWS. Authorities can initiate messages meant for dissemination over WEA by transmitting them to IPAWS-OPEN. They are then routed to cell towers within the designated area.



d heavy rains. Please refer to Columbia University homepage.

Emergency Alert

MANDATORY EVACUATION Zone A, Rockaways, Hamilton Bch, City Is. NYC.gov or 311 for details

Figure 2-3. WEA Message

Image courtesy of FEMA

WEA messages, as shown in Figure 2-3, can be generated for imminent threats (e.g., extreme weather), AMBER Alerts®, and Presidential alerts during national emergencies. Accompanied by vibration and a special tone to draw attention, these messages look similar to text messages but are broadcast to WEA-enabled cellular phones physically located in the alerting area at no charge to the recipient. WEA messages will be disseminated even when cellular networks are congested because different communication links are used. Citizens are not required to download an application or subscribe (i.e., "opt in") to a service in order to receive these messages. They can, however, opt out of any type of WEA except Presidential alerts.

According to the IPAWS Program Management Office (PMO), approximately 60 commercial wireless carriers currently participate in WEA. Information on WEA can be found on the IPAWS Website.

National Weather Service (NWS)

The NWS is a component of NOAA that provides weather, water, and climate data, forecasts and warnings for the protection of life and property and enhancement of the national economy. The All-Hazards Emergency Message Collection System, also known as "HazCollect," is a nationwide capability developed by the NWS, which automatically relays Non-Weather Emergency Messages (NWEMs) from NWS-approved officials to NWS dissemination systems including NOAA's All Hazards Weather Radio (NWR). Alerting authorities can leverage the NWR through IPAWS thereby adding additional pathways to reach the public. The NWS family of dissemination systems includes:

- NOAA Weather Radio All Hazards (NWR)—a network of radio stations nationwide with over 1,000 transmitters broadcasting continuous weather and timely emergency information;
- NOAA Weather Wire Service (NWWS)—a satellite data collection and distribution system that provides meteorological, hydrological, climatological, and geophysical

information to governmental and commercial emergency managers, media networks, and the public;

- Emergency Managers Weather Information Network (EMWIN)—a set of data access methods providing a live stream of weather and critical emergency information to emergency managers; and
- NWS Websites and Internet feeds such as the NWS home page.

Alerting authorities can request permission to send alerts through NWR by registering with the NWS. Before registering, the alerting authority must first complete the IPAWS application process. Then, the alerting authority can use IPAWS to send messages to NWS dissemination system transmitters via HazCollect. Messages are broadcast to all local NOAA Weather Radio All Hazards devices, such as those employed at schools for emergency purposes. An example of this type of radio is shown in Figure 2-4. EAS participants also monitor NWR and can broadcast messages received from their systems, providing even more robust alerting capability.

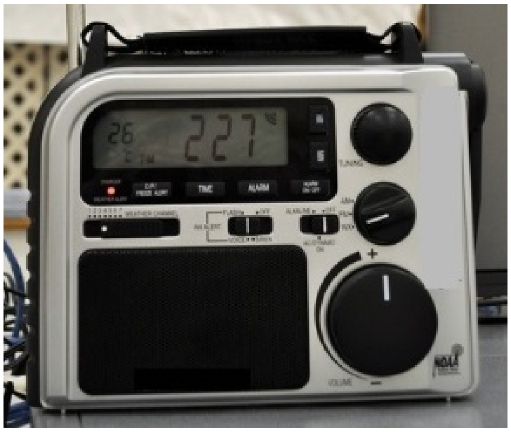


Figure 2-4. Weather Radio

Image courtesy of FEMA

Information on NWS dissemination systems can be found on the IPAWS Website.

2.2.4 Internet

The IPAWS Program supports alert and warning dissemination tools connected via the public Internet. When IPAWS-OPEN authenticates and validates a received message to be sent, it posts the message to the IPAWS All-Hazards Alert Feed. Web services and applications may request access to monitor this feed and retrieve applicable alert messages. They can display these messages on their websites through various display methods such as widgets, pop-ups, and RSS feeds. According to the IPAWS PMO, approximately 45 vendors currently have access to monitor the IPAWS All-Hazards Alert Feed. An example of a website that interfaces with alerting feeds is Google.org Public Alerts, which publishes alerts from sources including NWS, United States Geological Survey (USGS), and NCMEC. More information on how IPAWS uses Internet services to disseminate alerts can be found on the IPAWS Website.

The following are possibilities for redistribution of alerts:

- Websites and applications;
- Applications accessing social media sites;
- Computer and smartphone applications;
- Online gaming systems; and
- Instant messaging applications.

2.2.5 Unique Alerting Systems

CAP Alert Origination Tools can be used to disseminate CAP messages over public alerting systems already in use at state, local, territorial, and tribal levels. As long as these systems can communicate through the Internet and are CAP compliant, the systems can be programmed to interoperate with IPAWS for alerting functions. Upon receipt of a relevant CAP message through the network, the systems convert the message data into the form suitable for their technology (i.e., synthesized voice on radio and telephone, an appropriate signal on sirens). Unique alerting systems, two of which are shown in Figure 2-5, may include:

- Siren and public address systems;
- Emergency telephone networks;
- Land mobile radio systems;
- Digital road signs;
- Radio display in vehicles; and
- Mass SMS and e-mail notification systems.

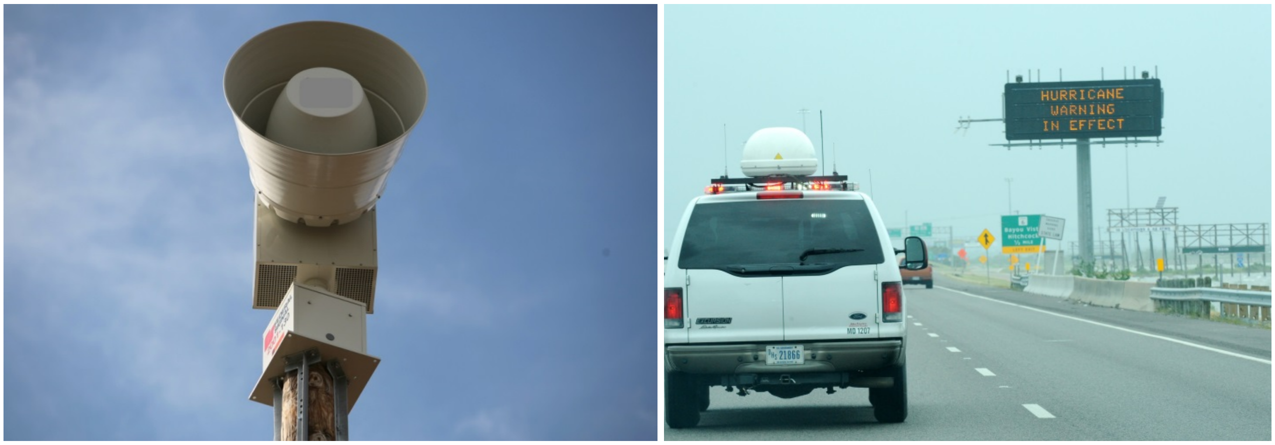


Figure 2-5. Siren and Digital Road Sign

Images courtesy of FEMA

More information on unique alerting systems can be found on the IPAWS Website.

2.2.6 End-User Devices

End-user devices are used to present alerts to the public through visual and auditory means. These devices include radios and televisions for messages disseminated by EAS; cellular phones for WEA messages; smartphones for mobile applications; NWR devices; computers and mobile devices for Internet communications; and devices such as sirens, digital road signs, and emergency radios.

3. CAP ALERT ORIGINATION TOOLS

CAP Alert Origination Tools are software programs designed to allow alerting authorities to create alert and warning messages in a consistent format for routing to multiple alerting systems. Many tools are commercially available for implementation in local jurisdictions. According to FEMA, there are approximately 80 vendors who have developed or are developing tools for use with IPAWS. Some agencies may determine that their current emergency communications system is already IPAWS compatible or can be made compatible with a vendor upgrade. Other agencies may need to acquire a tool.

3.1 Alert Origination Service Providers

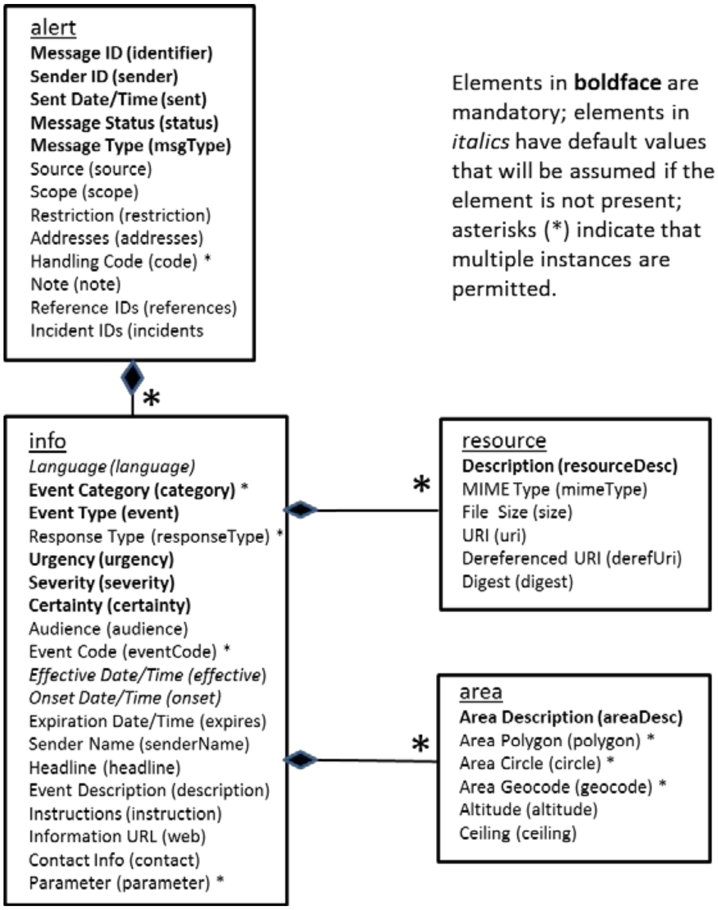
Alert Origination Service Providers are private and public sector organizations who furnish the CAP Alert Origination Tools to alerting authorities for the creation of CAP messages. Providers must execute a Memorandum of Agreement (MOA) with FEMA in order to access the IPAWS-OPEN environment for testing of their software. Upon completion of the MOA process, providers receive design guidance, a digital certificate, and an accessible web service end point with which to conduct testing in conjunction with the IPAWS PMO. A list of vendors who have an MOA in place with FEMA is available at the Alert Origination Service Providers Section of the IPAWS Website.

Agencies seeking to implement a CAP Alert Origination Tool should refer to the IPAWS Website for the requirements developers must meet to ensure a prospective tool has demonstrated compliance with the standards and protocols used for IPAWS. Information available includes lists of providers who have applied for an MOA to use the IPAWS test environment and providers that have received a declaration of conformance certifying that their tool is IPAWS compatible from initial testing and certification efforts (see Section 5). In addition, tool demonstration webinars are available at the IPAWS Website.

3.2 Messaging Protocols

CAP Alert Origination Tools use CAP as the messaging protocol for creation and processing of an IPAWS alert. CAP, based on Extensible Markup Language (XML), is an industry standard format for exchanging emergency alerts simultaneously between multiple alerting technologies. The CAP standard ensures that CAP messages share the same format regardless of the tool used to create the message. CAP messages always contain text, but can also contain audio, video, and geolocation data.

CAP messages, as shown in Figure 3-1, are formatted with one alert segment that may contain one or more info segments, each of which may contain one or more area and resource segments.



Elements in **boldface** are mandatory; elements in *italics* have default values that will be assumed if the element is not present; asterisks (*) indicate that multiple instances are permitted.

Figure 3-1. Structure of a CAP Message

Courtesy of OASIS®

- Alert segment—contains information on the following:
  - Unique message identifier;
  - Date/time stamp;
  - Status, such as “Actual”;
  - Type of message, such as “Alert” or “Test”;
  - Source, such as a county emergency operations center (EOC); and
  - Scope, such as “Public” or “Private”.
- Info segment—describes the event in terms of:
  - Category, such as “CBRNE” for a chemical, biological, radiological, nuclear, or explosive emergency;
  - Response type, such as “Evacuate”;
  - Urgency, such as “Immediate”;

  - Severity, such as “Moderate”;
  - Certainty, such as “Likely”;
  - Description of the emergency; and
  - Instructions for appropriate response.
- Resource segment—provides an optional reference to additional information such as an image or audio file.
- Area segment—describes the geographic area of the event in terms of:
  - Area description, such as postal code(s);
  - Geospatial shapes;
  - Geocodes;
  - Altitude; and
  - Ceiling.

3.3 Operation

A CAP Alert Origination Tool is most effective when it has an intuitive graphical user interface (GUI) to assist agencies in creating consistently formatted, CAP compliant messages. The IPAWS PMO provides many resources for agencies selecting and implementing tools, including best practices guides, frequently asked questions lists, fact sheets, and IPAWS implementation guidance.

According to the CAP v1.2 IPAWS Profile, conformance is achieved when:

- The tool (serving as a Message Producer) produces an XML document that conforms to the CAP v1.2 specification and the additional requirements outlined in the CAP v1.2 IPAWS Profile and;
- The tool (serving as a Message Consumer) validates the incoming message successfully.

Tools can also provide a number of capabilities, for example:

- Verify and display connectivity with IPAWS;
- Retrieve message status to verify the alert was successfully transmitted to the intended audience;
- Exchange messages with other IPAWS users;
- Format messages for dissemination to various public alerting systems, including the Internet and unique systems;
- Select public alerting system;
- Designate geographic area of message on a map with a polygon;
- Accommodate 90 character text (WEA only);

- Accommodate multiple languages;
- Provide templates for message creation;
- Verify connectivity/acknowledgement of successful transmission;
- Parse IPAWS EAS Feed and/or IPAWS All-Hazards Alert Feed;
- Filter alerts by selected geography, alert type, current geographical location, or other criteria;
- Support attachments (i.e., audio, video, image); and
- Support fetching content via URL in CAP (i.e., audio, video, image).

3.4 Acquisition Considerations

Agencies must determine the extent of the integration of the selected messaging tool into their information technology (IT) infrastructure and communications environment. Cost and security are also important considerations.

3.4.1 Systems/Architecture Considerations

Integrating a CAP Alert Origination Tool into an agency's systems and IT architecture should be planned carefully. When considering the acquisition of a new CAP tool, two major options are available. The first is acquisition of a new emergency management system and the second is to upgrade an existing system with new capabilities. Each method has its own considerations, but both require a careful evaluation of IT requirements.

As with all IT acquisitions, pre-planning can help avoid considerable difficulties during implementation. The agency should understand the requirements of the new CAP tool and functionality, including hardware requirements, software requirements (e.g., operating systems), and interaction with existing IT policies.

The simplest option for acquisition is to acquire a stand-alone CAP Alert Origination Tool. The primary benefit of this option is that there are no costs or issues arising from integrating the tool into other agency systems. This gives the acquiring agency considerable freedom to select a tool that best fits their needs and budget. However, the lack of integration into existing emergency management systems means that an additional staff resource may be needed to operate the tool.

Acquiring a new CAP Alert Origination Tool for integration into an agency's existing systems is another option. This offers the ability to use the CAP tool within the existing alerting plans, and requires a smaller investment in training in exchange for more effort on the integration. Given the number of potential configurations, specific integration guidance is difficult to define; however, there are a few common considerations. When integrating systems, an important consideration is the method used to trade information. It is preferable to acquire a new system that is compatible with an agency's existing systems. This is not always possible and a translation application may be necessary to convert information from existing systems to the CAP tool and vice versa. Translation applications are often custom designed for the systems in question, so agencies should be prepared to negotiate with the vendor or a third party when making acquisition plans.

An upgrade can consist of software and/or hardware updates that can provide CAP Alert Origination Tool functionality. If an update to existing systems exists, this provides another option besides acquiring a new system. Updating existing systems allows the agency to preserve existing investments and training, and can provide a cost savings over acquiring a new system. The agency should investigate what the update requires, as some updates alter the existing interfaces or functionalities of the system.

Finally, an agency may choose to replace their existing emergency management systems with a new system that includes a CAP Alert Origination Tool. This is a major undertaking, and should be considered carefully. It may be a good option if the existing systems are dated or insufficient for agency needs and the agency has the budget for the acquisition.

Best practices related to upgrades include implementing the system on a test platform first to identify any issues prior to putting the system into operation. If this is not feasible, the agency should consider having upgrades performed by qualified vendor personnel (or by agency IT resources with vendor personnel available) in order to be able to best respond to any unintended effects of the upgrade. Backing up the existing system in a format that can be redeployed is a good practice to preserve continuity of operation, in case the upgrade fails.

3.4.2 Cost Considerations

Regardless of how an agency integrates a CAP Alert Origination Tool into their system architecture, several considerations for ongoing costs are universal. The IPAWS PMO mandates training for all agencies prior to gaining access to IPAWS. Regular training (for IPAWS and the CAP tool itself) is recommended and should be incorporated into training plans and budgets. If applicable, agencies should consider the cost of staff time to update standard operating procedures as a result of the tool's integration with other alerting systems. Some tools may have annual software licensing costs, and hardware maintenance and replacement costs should be considered.

The FEMA MOA process introduces some costs to consider as well. These include staff time for:

- The IPAWS application process;
- Alert authority approval process;
- Coordination with surrounding alerting agencies;
- Functional testing of the tool and its integration with existing alerting systems; and
- Development or revision of alerting plans.

The IPAWS PMO published the *Integrated Public Alert and Warning (IPAWS) Fiscal Year 2014 Supplemental Guidance on Public Alert and Warning* to help prospective grantees understand the public alert and warning projects eligible for Federal grant funding. The document can be found at the Informational Materials Section of the IPAWS Website. The IPAWS PMO offers guidance, tools, and resources to any agency planning to initiate grant activities for IPAWS implementation. The following grant programs can be used to establish new alert and warning capabilities or enhance existing systems:

- Homeland Security Grant Program (HSGP); and
- Tribal Homeland Security Grant Program (THSGP).

3.4.3 Security Considerations

One of the primary concerns regarding public alerting is the potential for the issue of contradictory, redundant, or fake emergency messages. This situation has the potential to create confusion or panic for emergency responders and the public during stressful times. Prior to being granted access to IPAWS, each alerting authority signs an IPAWS MOA and Rules of Behavior, which outline the access control, proper use, password complexity, safeguarding of credentials, accountability, and incident reporting requirements. Failure to adhere to these fundamental security practices may result in loss of access and civil or criminal prosecution. Regarding IPAWS, security breaches can result in revocation of the agency's agreement with FEMA, as defined in the IPAWS MOA and Rules of Behavior signed by the alerting authority.

Security considerations and best practices for CAP Alert Origination Tools include careful management of email addresses, user accounts, and physical devices/computers used to access IPAWS. Agencies should designate IPAWS users with a level of access commensurate with their roles and authority. Agencies can implement sound password security practices, such as password strength requirements, periodic prompts to change the password, and limitations on repeating passwords. Access to physical devices used for IPAWS should be limited and approved. These devices should be protected; for example, the computer may be located in the EOC with an access control system in place. Agencies can also recommend that users complete security awareness training.

Additional information regarding the acquisition of IPAWS Compliant CAP Alert Origination Tools can be found in the *Study of Integration Strategy Considerations for Wireless Emergency Alerts* report and the *Wireless Emergency Alerts (WEA) Cybersecurity Risk Management Strategy for Alert Originators* report located in the Document Library on FirstResponder.gov.

4. STANDARDS AND TECHNICAL RESOURCES

The IPAWS PMO has published many documents that can be valuable resources to implementing agencies, and are available on the Informational Materials Section of the IPAWS Website. All agencies utilizing IPAWS must deploy equipment and software that conforms to standards described in Sections 4.1 through 4.4.

4.1 CAP Messaging Standard

IPAWS uses CAP, an internationally recognized XML messaging standard approved by the Organization for the Advancement of Structured Information Standards (OASIS®) and adopted by FEMA in 2010. The most current version is the *OASIS Common Alerting Protocol Version 1.2*, also called CAP v1.2, which can be found at the OASIS Website. Open and non-proprietary, the CAP format is compatible with existing formats used by national public alerting systems as well as Internet services and unique systems used by alerting authorities. CAP also provides additional capabilities such as geographic targeting of the dissemination area, multilingual messaging, and attachment of images and audio.

4.2 CAP IPAWS Profile

IPAWS alert messages must also conform to the CAP v1.2's companion document, the *OASIS Common Alerting Protocol, v. 1.2 USA Integrated Public Alert and Warning System Profile Version 1.0.* Typically referred to as the CAP v1.2 IPAWS Profile, this document provides additional specifications for conformance to the CAP standard necessary to meet the needs of IPAWS participants and providers. The CAP v1.2 IPAWS Profile:

- Integrates requirements of the EAS, HazCollect, and WEA systems;
- Specifies the constraints that the CAP IPAWS Profile places on the CAP message in order for the message to be IPAWS compatible; and
- Provides conformance requirements for the CAP message, the CAP origination software, and the CAP destination software.

The CAP v1.2 IPAWS Profile can be found at the OASIS Website.

4.3 CAP EAS Implementation Guide

Because alerts disseminated over EAS can be encoded in various ways, there can be a difference between the intended message and the one that is ultimately broadcast by CAP/EAS devices. The EAS-CAP Industry Group (ECIG), formed by EAS equipment providers and other interested parties in 2008, met to develop a set of recommendations for EAS participants in order to promote interoperability at a data and messaging level. Their document, *ECIG Recommendations for a CAP EAS Implementation Guide* provides guidance for successful transmission of CAP messages through the EAS to the public, regardless of the vendors or platforms involved. The document can be found at the ECIG Documents Section of the ECIG Website.

4.4 Code of Federal Regulations Title 47 Parts 10 and 11

Part 10 of the FCC's rules and regulations focuses on the WEA system and describes the requirements for participation. The document can be found at the Code of Federal Regulations (CFR) Website. Requirements of Part 10 include:

- The Election to Participate procedures, which outline the steps Commercial Mobile Service Providers (or CMS Providers) take to participate in the WEA system inclusive of providers that elect to not transmit WEA alert messages;

- Specific language to be used by CMS Providers to notify consumers of their participation level (e.g., fully, partially, or do not participate) inclusive of Point of Sale notifications;
- The conditions under which a consumer can opt out; and
- The equipment, alert message, and testing requirements.

Part 11 of the FCC's rules and regulations focuses on the EAS. It describes the technical standards and operational procedures that EAS participants must follow in order to comply with EAS rules. The document can be found at the Code of Federal Regulations (CFR) Website. Requirements of Part 11 include:

- The equipment, such as EAS decoders and encoders, that must be deployed and operational at EAS Participant locations;
- The EAS Operating Handbook provided by the FCC, which details the actions that must be taken by EAS participants upon receipt of Presidential alerts, EAS alerts, tests, or state/local area alerts;
- State and local area EAS Plans submitted to the FCC specifying guidelines to be followed by EAS participants' personnel, emergency officials, and NWS personnel to activate the EAS; and
- The FCC Mapbook, which organizes all EAS participants according to state, local area, and EAS designation, based on EAS plans.

4.5 IPAWS Toolkit for Alerting Authorities

The *IPAWS Toolkit for Alerting Authorities* is a FEMA resource that can help emergency managers incorporate IPAWS into their alerting plans. The document provides information on adopting CAP and ensuring the community is made aware of the types of alerting methods that are employed and how to access, use, and respond to them. This document, along with various fact sheets and frequently asked questions, can be found at the Informational Materials Section of the IPAWS Website. Additionally, Appendix B, IPAWS Implementation Guidelines, contains a summary of the steps agencies need to take in order to gain access to IPAWS.

5. TESTING AND CERTIFICATION

CAP-capable equipment, systems, and software must be IPAWS compatible according to the FCC and IPAWS PMO standards and requirements. Conformance can be demonstrated through several testing and demonstration programs, as explained below. Agencies implementing a CAP Alert Origination Tool must ensure that the vendor they select has tested and certified their products' IPAWS compatibility.

5.1 IPAWS Conformity Assessment Program

The IPAWS PMO managed a testing program that concluded in August 2011 called Conformity Assessment (CA), and a Supplier's Declaration of Conformity (SDoC) was issued to many vendors. The program provided an independent, objective analysis of qualified products conducted in an accredited lab to ensure the product adhered to the CAP IPAWS Profile.

Products were tested for conformance to CAP v1.2, the CAP IPAWS Profile, the ECIG CAP EAS Implementation Guide, and FCC Title 47 of the CFR Part 11. Conformance was documented in SDoCs, which vendors could then use to obtain or update their FCC certification and gain access to IPAWS for their customer. A listing of tools that were issued SDoCs can be found on the Certifications and Declarations Section of the Lessons Learned Information Sharing Website.

5.2 P-TAC STEP Program

FEMA's Preparedness-Technology, Analysis, and Coordination (P-TAC) Center also managed a testing program, ending in September 2013, called the Supporting Technology Evaluation Project (STEP). SDoCs were issued to vendors as a result of the testing. The P-TAC Center houses an EOC test environment and accredited laboratory. A number of CAP Alert Origination Tools were tested under STEP for conformance to the CAP IPAWS Profile, the CAP EAS Implementation Guide, and FCC Title 47 of the CFR Part 11.

5.3 Independent Testing Authority

Vendors can use an independent, accredited testing authority to conduct testing of their product. In order to assist in this effort, FEMA published the *Integrated Public Alert and Warning System (IPAWS) Guide for Independent Testing of Emergency Alert System Equipment* that describes the requirements for testing CAP-capable devices or software for conformance. The document and other information on independent testing can be found on the IPAWS Website. Upon completion of testing, a copy of the results can be submitted to the FCC.

5.4 Demonstration Webinars

In an effort to keep abreast of vendor efforts to test and certify their products' IPAWS compatibility, the IPAWS PMO initiated a webinar series in 2013 to provide vendors a platform on which to demonstrate their products' ability to interface with IPAWS. These webinars can be helpful for vendors and emergency responder agencies to gain familiarity with various tools and their capabilities. Agencies can join working groups, subscribe to the webinar e-mail list, or view past webinars using resources listed on the IPAWS Website.

5.5 IPAWS Testing Lab

The FEMA-supported IPAWS Demonstration and Test center, operated by the Joint Interoperability Test Command (JITC) under the Department of Defense (DoD) Defense Information Systems Agency (DISA), maintains the IPAWS testing laboratory. The lab provides support for the IPAWS PMO, Alert Origination Service Providers, and alerting authorities for tool assessments, demonstrations, exercises, and testing. As agencies execute the steps required to use IPAWS, they will work with the IPAWS PMO and JITC to test their systems prior to going live. See Appendix B for more information on functional testing at JITC.

6. SUMMARY

IPAWS is a continually evolving dissemination system for national and local emergency alerts. Emergency responder agencies can take advantage of IPAWS capabilities, including sending alerts over multiple public alerting systems simultaneously, by using a CAP Alert Origination Tool. These tools provide the capability to create consistent, IPAWS compatible messages based on the CAP standard. Many agencies may already have a tool in place in their alerting system architecture and others need to work with vendors to purchase and install one.

FEMA provides assistance to emergency responder agencies connecting to IPAWS. Guidelines, standards, advice, fact sheets, and frequently asked questions lists are available on the FEMA Website. The IPAWS PMO is also actively involved in helping vendors test their tools and equipment for IPAWS compatibility. The purpose of this technology guide was to consolidate information found in a wide variety of locations into a single document, in order to assist emergency responder agencies who are planning to purchase and implement a CAP Alert Origination Tool as part of their alerting solution.

7. REFERENCES

DHS. Certifications and Declarations. https://www.llis.dhs.gov/knowledgebase/certifications-declarations-list (accessed October 8, 2014).

EAS-CAP Industry Group. *ECIG Recommendation for a CAP EAS Implementation Guide*. http://www.eas-cap.org/ECIG-CAP-to-EAS_Implementation_Guide-V1-0.pdf (accessed April 17, 2014).

FCC. Part 11-Emergency Alert System (EAS). http://www.ecfr.gov/cgi-bin/text-idx?SID=6018d3a8d6d75f385285e4189c967caa&node=47:1.0.1.1.12&rgn=div5 (accessed November 4, 2014).

FEMA. Alerting Authorities. http://www.fema.gov/integrated-public-alert-warning-system-authorities (accessed October 25, 2014).

FEMA. Alert Origination Service Providers. http://www.fema.gov/alert-origination-service-providers (accessed October 17, 2014).

FEMA. Common Alerting Protocol. http://www.fema.gov/common-alerting-protocol (accessed April 17, 2014).

FEMA. Developer Webinars. https://www.fema.gov/alert-origination-service-providers#3 (accessed October 8, 2014).

FEMA. EAS. http://www.fema.gov/emergency-alert-system (accessed October 8, 2014).

FEMA. EMI Independent Study Program. http://training.fema.gov/IS (accessed October 8, 2014).

FEMA. *Fiscal Year 2014 Supplemental Grant Guidance on Public Alert and Warning*. https://s3-us-gov-west-1.amazonaws.com/dam-production/uploads/1398964784842-51f628731cbd3320c41ae8e73def4f85/FY+2014+Supplemental+Guidance_Integrated+Public+Alert+and+Warning+Guidance.pdf (accessed April 14, 2014).

FEMA. Homepage. http://www.fema.gov/integrated-public-alert-warning-system (accessed November 6, 2014).

FEMA. How to Sign Up for IPAWS. http://www.fema.gov/how-sign-ipaws (accessed November 6, 2014).

FEMA. Independent Testing. http://www.fema.gov/media-library-data/20130726-1836-25045-2590/ipaws_eas_testing_guide_201206.pdf (accessed May 8, 2014).

FEMA. Informational Materials. http://www.fema.gov/informational-materials (accessed November 6, 2014).

FEMA. Integrated Public Alert and Warning System Working Groups. http://www.fema.gov/integrated-public-alert-and-warning-system-working-groups (accessed May 8, 2014).

FEMA. Internet Services. http://www.fema.gov/internet-service-providers (accessed April 18, 2014).

FEMA. IS-251: Integrated Public Alert and Warning System (IPAWS) for Alerting Authorities. http://emilms.fema.gov/IS0251/IPAWS03summary.htm (accessed October 8, 2014).

FEMA. IPAWS Architecture Diagram. http://www.fema.gov/media-library/assets/documents/26592 (accessed October 3, 2014).

FEMA. IPAWS–OPEN. http://www.fema.gov/integrated-public-alert-warning-system-open-platform-emergency-networks (accessed October 17, 2014).

FEMA. IPAWS Presentation at Governors' Hurricane Conference, May 13, 2014. http://flghc.org/ppt/2014/Training%20Sessions/TS36%20Emerg%20Comms%20Support/TS36/20140513%20IPAWS%20for%20Gov%27s%20Hurricane%20Conf%20Session%20TS36%20with%20vid%20clip.pdf (accessed November 6, 2014).

FEMA. *IPAWS Toolkit for Alerting Authorities*. http://www.fema.gov/media-library-data/1386178113188-5c307e810a273fd349cacbc2e641df76/IPAWS+Toolkit+for+Alerting+Authorities_11122013_FINAL.pdf (accessed November 6, 2014).

FEMA. MOA Application. https://s3-us-gov-west-1.amazonaws.com/dam-production/uploads/1394045827417-0e620ec29502082a06640b95d1249325/IPAWS-OPEN+Operational+COG+Application+Template_20140224+(2).pdf (accessed May 5, 2014).

FEMA. National Weather Service Systems. https://www.fema.gov/national-weather-service-systems-noaa-hazcollect (accessed November 6, 2014).

FEMA. P-TAC Center. STEP Testing. https://www.ptaccenter.org/step/index (accessed May 8, 2014).

FEMA. Private Sector Alert Origination Service Providers. http://www.fema.gov/integrated-public-alert-warning-system-private-sector (accessed October 17, 2014).

FEMA. Unique Systems. http://www.fema.gov/unique-systems (accessed April 18, 2014).

FEMA. WEA. http://www.fema.gov/wireless-emergency-alerts (accessed October 8, 2014).

National Radiological Emergency Preparedness Conference, Inc. IPAWS Presentation, April 26, 2012. http://www.nationalrep.org/2012Presentations/Session%2024_FEMAs%20Integrated%20Public%20Alert%20and%20Warning%20System%20%28IPAWS%29_Witmer.pdf (accessed April 22, 2014).

OASIS. *OASIS Common Alerting Protocol Version 1.2*. http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2-os.pdf (accessed April 17, 2014).

OASIS. *OASIS Common Alerting Protocol, v. 1.2 USA Integrated Public Alert and Warning System Profile Version 1.0.* http://docs.oasis-open.org/emergency/cap/v1.2/ipaws-profile/v1.0/cap-v1.2-ipaws-profile-v1.0.pdf (accessed April 17, 2014).

Software Engineering Institute. Best Practices in Wireless Emergency Alerts, September 2013. http://www.firstresponder.gov/TechnologyDocuments/Wireless%20Emergency%20Alerts%20Best%20Practices.pdf (accessed October 14, 2014).

Software Engineering Institute. Study of Integration Strategy Considerations for Wireless Emergency Alerts, September 2013. http://www.firstresponder.gov/TechnologyDocuments/Wireless%20Emergency%20Alerts%20Integration%20Strategy.pdf (accessed October 14, 2014).

Software Engineering Institute. Wireless Emergency Alerts (WEA) Cybersecurity Risk Management Strategy for Alert Originators, September 2013. http://www.firstresponder.gov/TechnologyDocuments/Wireless%20Emergency%20Alerts%20Cybersecurity%20Risk%20Management%20Strategy%20for%20Alerts%20Originators.pdf (accessed October 14, 2014).

Texas Department of Public Safety. IPAWS Presentation at the Texas Emergency Management Conference, May 14, 2014. https://www.preparingtexas.org/Resources/documents/2014%20TEMC/IPAWS%20-%20Get%20Alerts%20-%20Stay%20Alive.pdf (accessed October 14, 2014).

APPENDIX A. ABBREVIATIONS AND ACRONYMS

Acronym	Description
AEL	Authorized Equipment List
AMBER	America's Missing: Broadcast Emergency Response
CA	Conformity Assessment
CAP™	Common Alerting Protocol
CBRNE	Chemical, Biological, Radiological, Nuclear, and Explosive
CFR	Code of Federal Regulations
CMAS	Commercial Mobile Alert System
COG	Collaborative Operating Group
DHS	U.S. Department of Homeland Security
DISA	Defense Information Systems Agency
DoD	Department of Defense
EAS	Emergency Alert System
ECIG	EAS-CAP Industry Group
EMI	Emergency Management Institute
EMWIN	Emergency Managers Weather Information Network
EOC	Emergency Operations Center
ETN	Emergency Telephone Network
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
GUI	Graphical User Interface
HazCollect	All-Hazards Emergency Message Collection System
HSGP	Homeland Security Grant Program
ID	Identification
IP	Internet Protocol
IPAWS-OPEN	Integrated Public Alert and Warning System—Open Platform for Emergency Networks
IT	Information Technology
JITC	Joint Interoperability Test Command
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NCMEC	National Center for Missing and Exploited Children

Acronym	Description
NOAA	National Oceanic and Atmospheric Administration
NWEM	Non-Weather Emergency Messages
NWR	NOAA Weather Radio
NWS	National Weather Service
NWWS	NOAA Weather Wire Service
OASIS®	Organization for the Advancement of Structured Information Standards
PEP	Primary Entry Point
PMO	Program Management Office
P-TAC	Preparedness-Technology, Analysis, and Coordination
RBDS	Radio Broadcast Data Systems
SAME	Specific Area Message Encoding
SAVER	System Assessment and Validation for Emergency Responders
SDoC	Supplier's Declaration of Conformity
SMS	Short Message Service
SPAWARSYSCEN	Space and Naval Warfare Systems Center
STEP	Supporting Technology Evaluation Project
THSGP	Tribal Homeland Security Grant Program
USGS	United States Geological Survey
VHF	Very High Frequency
WEA	Wireless Emergency Alerts
XML	Extensible Markup Language

APPENDIX B. IPAWS IMPLEMENTATION GUIDELINES

Agencies must follow a series of steps, highlighted on the Integrated Public Alert and Warning System (IPAWS) IPAWS Website in order to gain access to IPAWS. Information on agencies who are currently using IPAWS or who are in the process of implementing IPAWS can be found on the IPAWS Website. The requirements for IPAWS implementation ensure that emergency messages from the President are disseminated accurately and effectively, and that national public alerting systems are used to send and receive messages in accordance with the Federal Communications Commission (FCC)'s rules and regulations. The steps are summarized in Figure B-1.

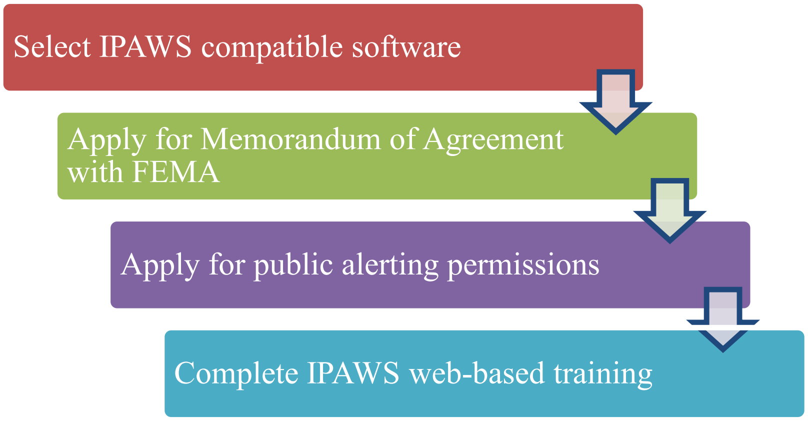

Select IPAWS compatible software
Apply for Memorandum of Agreement with FEMA
Apply for public alerting permissions
Complete IPAWS web-based training

Figure B-1. Steps for Signing Up for IPAWS

Image courtesy of FEMA

Participation Requirements

Any qualifying public safety organization, recognized by appropriate Federal, state, local, territorial, or tribal alerting authorities, may apply for authorization to use IPAWS. Basic technical requirements include an Internet connection and an IPAWS compatible software system.

Collaborative Operating Groups

A Collaborative Operating Group (COG) is "established when a Federal, state, local, territorial, or tribal alerting authority successfully applies for authorization to use IPAWS. A COG may have members from multiple organizations (e.g., a regional mutual aid organization)."[1] The COG is designated during the IPAWS approval process and can be a single agency or a group of agencies.

These groups can be helpful in coordinating the issue of alerts across a local area or neighboring areas: "One of the unique features is that COGs can foster communication, collaboration, and coordination not only during the incident response phase, but also in regard to incident preparedness, mitigation, and recovery. COGs can be set up to allow for COG-to-COG

[1] DHS FEMA IPAWS. *IS-251: Integrated Public Alert and Warning System (IPAWS) for Alerting Authorities*. http://emilms.fema.gov/IS0251/IPAWS03summary.htm (accessed July 8, 2014).

messaging that promotes increased collaboration or in addition to messaging COG-to-COG, they also have alerting permission to send alert messages to the public. COGs consist of, but are not limited to, organizations such as local fire departments, offices of emergency management, state police, and public universities." [2] Multiple agencies (e.g., fire departments and police departments) may be authorized alerting authorities and can potentially issue contradictory alerts. Membership in a managed COG would help avoid these situations through collaboration and coordination.

The Federal Emergency Management Agency (FEMA) cites that there is no one universal way in which to set up a COG; they should be set up based on needs and what works best for organizations and/or the state working to implement IPAWS. Irrespective of the COG structure, a Memorandum of Understanding (MOU) should be in place; MOUs outline the coordination and support required in order for a COG to function:

"MOUs and Memorandums of Agreement (MOAs) safeguard the confidentiality, integrity, and availability of the IPAWS software systems; ensure that the systems are deployed for official use only; and prevent duplicate, frivolous, and/or contradictory alerts from being disseminated to the public." [2]

A self-paced, online training course (IS-251) designed to increase awareness about COGs is provided through FEMA's Emergency Management Institute (EMI).

Approval Steps

The steps to be taken by agencies applying for IPAWS access are summarized below.

Step 1: Identify and Procure a Common Alerting Protocol (CAP) Alert Origination Tool that fits operational plans and use cases. The software developer must have executed an MOA with FEMA to develop IPAWS Open Platform for Emergency Networks (IPAWS-OPEN) compatible tools. Considerations for selection include the types of alerts that will be sent, messaging templates required, security mechanisms provided, and requirements for integration with existing tools. Other considerations are discussed in the *IPAWS Toolkit for Alerting Authorities*.

Step 2: Apply for an MOA with FEMA. Establishment of a COG requires execution of an MOA governing system security between the sponsoring organization and FEMA. Each MOA is specifically tailored to the sponsoring organization and their interoperable software system. The MOA application including instructions for completion, the email address for application submission, and the subject for the application email are located on the How to Sign Up for IPAWS Section of the IPAWS Website.

The FEMA COG coordinator will prepare and return the MOA to the sponsoring agency for signature. The MOA is then routed for FEMA signatures. Once executed, a COG Identification (ID) and digital certificate will be generated and implemented in IPAWS-OPEN. A copy of the executed MOA, the COG ID, and the digital certificate will be sent to the sponsoring organization. The digital certificate and COG ID is necessary to configure the IPAWS

[2] DHS FEMA IPAWS. *IS-251: Integrated Public Alert and Warning System (IPAWS) for Alerting Authorities.* http://emilms.fema.gov/IS0251/IPAWS03summary.htm (accessed July 8, 2014).

compatible software system. After completing these steps, the organization will have the capability to exchange standards-compliant messages and content between COGs.

Step 3: Apply for public alerting permissions from FEMA. Alerting authorities that want to send alerts to the public through IPAWS must complete an application defining the types of alerts they intend to issue and the extent of their geographic warning area. The application for IPAWS public alerting authority will be provided during the COG MOA application process, along with contact information for a designated state reviewer. In order to ensure consistency with Federal, state, local, territorial, and tribal alerting plans, the application must be reviewed and signed by a designated state (or appropriate) official before it is submitted to FEMA.

Step 4: Complete IPAWS web-based training. Agencies are required to complete the IS-247.A *Integrated Public Alert and Warning System* course. This self-paced, online training course is provided by FEMA's EMI.

After all requirements have been met, specific alerting permissions will be implemented in IPAWS-OPEN. At that point the individual members specified by the COG will be able to send alerts and warnings in the geographically prescribed areas.

Initial functionality includes the ability to access and send alerts through:

- The Emergency Alert System (EAS);
- The National Weather Service (NWS) All-Hazards Emergency Message Collection System for NWS-approved alerting authorities (once permission has been granted by National Oceanic and Atmospheric Administration [NOAA]); and
- Wireless Emergency Alerts (WEA), depending on local implementation by commercial mobile service providers.

Information on the approval steps and links to forms are available on the How to Sign Up for IPAWS Section of the IPAWS Website.

Functional Testing

Before, during, or after the above steps have been completed, alerting authorities are highly encouraged to seek assistance with testing through the IPAWS Program Management Office (PMO) and Joint Interoperability Test Command (JITC). The steps for testing include the following:

- Preparing to test—this ensures the functional requirements to be tested have been identified, the alerting authority has an IPAWS compatible software product installed and ready, a test plan has been created, and that JITC has copies of applicable manuals;
- Controlled environment testing—JITC staff executes the test plan and confirms all functional requirements are met; and
- Operational field assessment—this test is executed in the field in a real-world environment. Results are observed and documented and a final assessment report is delivered.

Other Recommended Actions

The IPAWS PMO also makes the following recommendations for local alerting authorities:

- Develop a Public Alerting Plan that documents local public alert standard operating procedures;
- Coordinate with local Primary Entry Point (PEP) stations for dissemination of alerts in state, local, territorial, and tribal disaster response when they are not being used for a national catastrophic emergency;
- Coordinate with the state emergency manager, state IPAWS representative, local EAS and NWS officials, and neighboring local jurisdictions about public alerting;
- Inform citizens about how and where alerts will be disseminated; and
- Practice—conduct training, drills, and exercises for receipt and transmission of alerts.

Additional Resources

Additional information regarding the implementation of IPAWS can be found in the *Best Practices in Wireless Emergency Alerts* report located in the Document Library on FirstResponder.gov.